vision

Cyber Security Awareness

Wyoming Office of the CIO

State IT Security Policy 141

Information Security Awareness and Training

- This policy establishes the requirement for information technology (IT) security awareness and training in all executive branch agencies.
- Security Awareness. All State employees shall be exposed to security awareness materials throughout the year.
- Recurring Training. All State employees shall receive an annual refresher that reinforces relevant information security issues.

http://cio.state.wy.us/standards/srce/web/default.htm

- Not sure where to go?

Federal Fast Access

- U.S. Government's Official Web Portal

USA.gov Government Made Easy

Helpful Links

- Wyoming Attorney General: Computer and High Tech Crimes
- Stay Safe Online.org
- MS-ISAC: Multi-State Information Sharing and Analysis Center
- MS-ISAC: Cyber Security Awareness
- US Office of Homeland Security: Cyber Security - Make it a Habit
- US Office of Homeland Security: National Cyber Security Awareness Month
- U.S. Cert: Security Publications

View the Governor's proclamation

MS-ISAC Cyber Tip:

What info is collected when you visit a

Printable Awareness Materials

Safe Kids

- Safe Kids Links
- Internet Safe Kids Pledge
- Cyber Security Awareness Volunteer Education Program (C-SAVE) Fact Sheet
- K-12 Educators Lesson Plans

Publications

- Executive Brief: Information Security
- How-To-Guide for IT Security in Government
- Getting Started: A Non-Technical Guide for Executives and Managers
- Brief: State of Enterprise Security 2010
- Security Newsletter - Backing Up Your Files
- Security Awareness Presentation
- Security Awareness Quiz

Security News

Vuln Orbital Viewer .orb File Stack-Based Buffer Overflow Vulnerability

Technical Theatre Agenda

Business Strategy Theatre Agenda

NEW - The Discussion Den Theatre

Keynote Theatre Agenda

NA - CVE-2009-4677 - Cross-site scripting XSS vulnerability in...

NA - CVE-2009-4678 - Cross-site scripting XSS vulnerability in...

NA - CVE-2009-4679 - Directory traversal vulnerability in the...

Latest Vulnerabilities

Provided by SecurityTracker

Energizer DUO Charger USB Software Contains Trojan Software That Lets Remote Users Execute Arbitrary Code

SpamAssassin Milter Plugin Input Validation Flaw Lets Remote Users Execute Arbitrary Code

Opera Integer Overflow in Processing HTTP 'Content-Length' Reponses Lets Remote Users Execute Arbitrary Code

Juniper Instant Virtual Extranet (IVE) Input Validation Hole in 'editbk.cgi' Permits Cross-Site Scripting Attacks

Don’t Be a Billy

- http://www.youtube.com/watch?v=nPR131wMKEo

Social Engineering (tactics)

- A non-technical kind of intrusion, rather than by breaking in or using technical hacking techniques
- Relies heavily on human interaction
- Tricking or manipulating people into performing actions or divulging confidential information

Social Engineering (tactics)

- Pretexting – invented scenario
- Diversion theft – intercepting a consignment
- Interactive Voice Response (IVR) – fake phone tree
- Baiting – dropped USB stick
- Quid pro quo – random calling
- Phishing – fraudulent email

Phishing

- The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- Typically carried out by e-mail or instant messaging

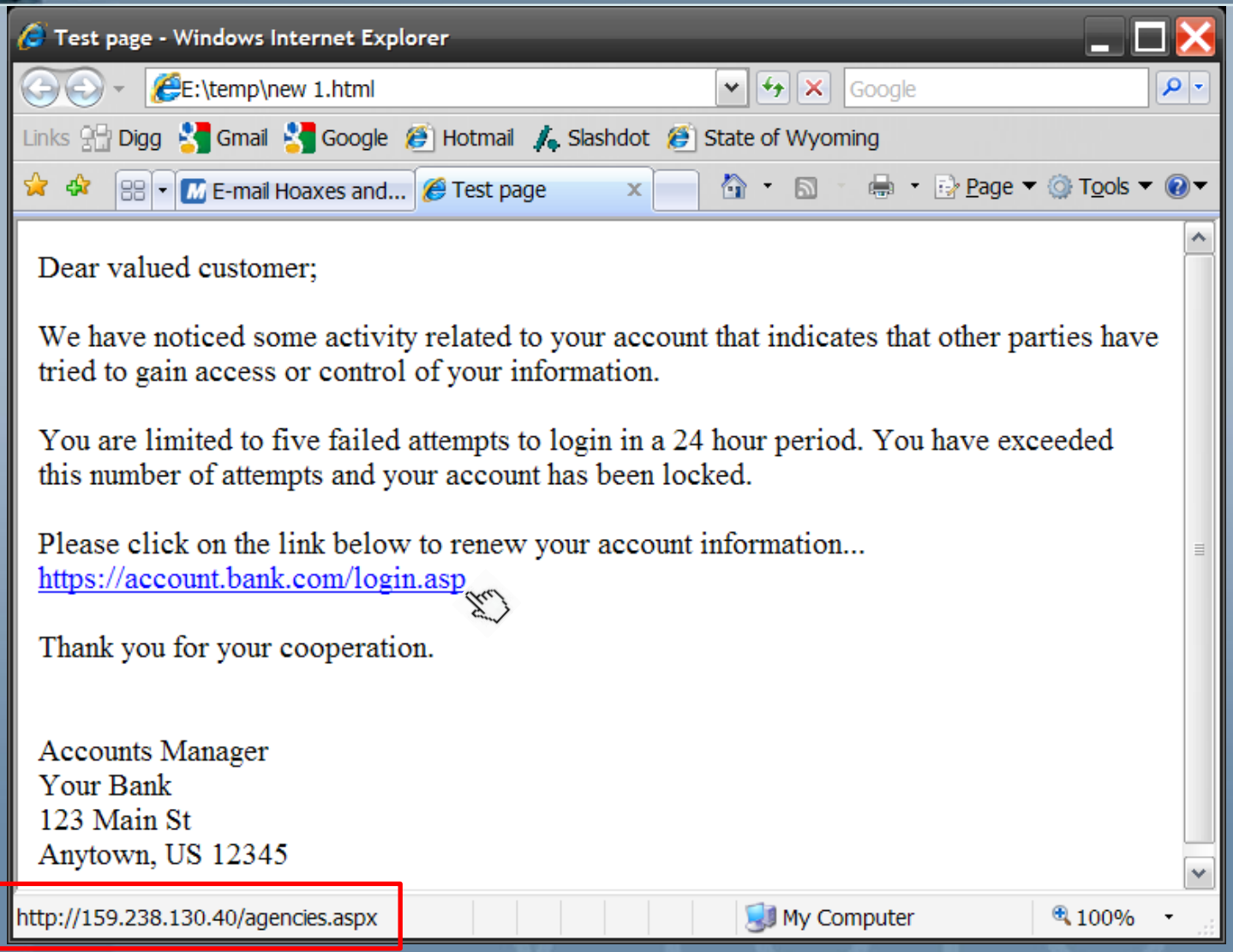
Phishing

- Methods used to lure the unsuspecting:
  - social web sites
  - auction sites
  - online payment processors
  - IT administrators
- Often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Difficult to detect that the website is fake

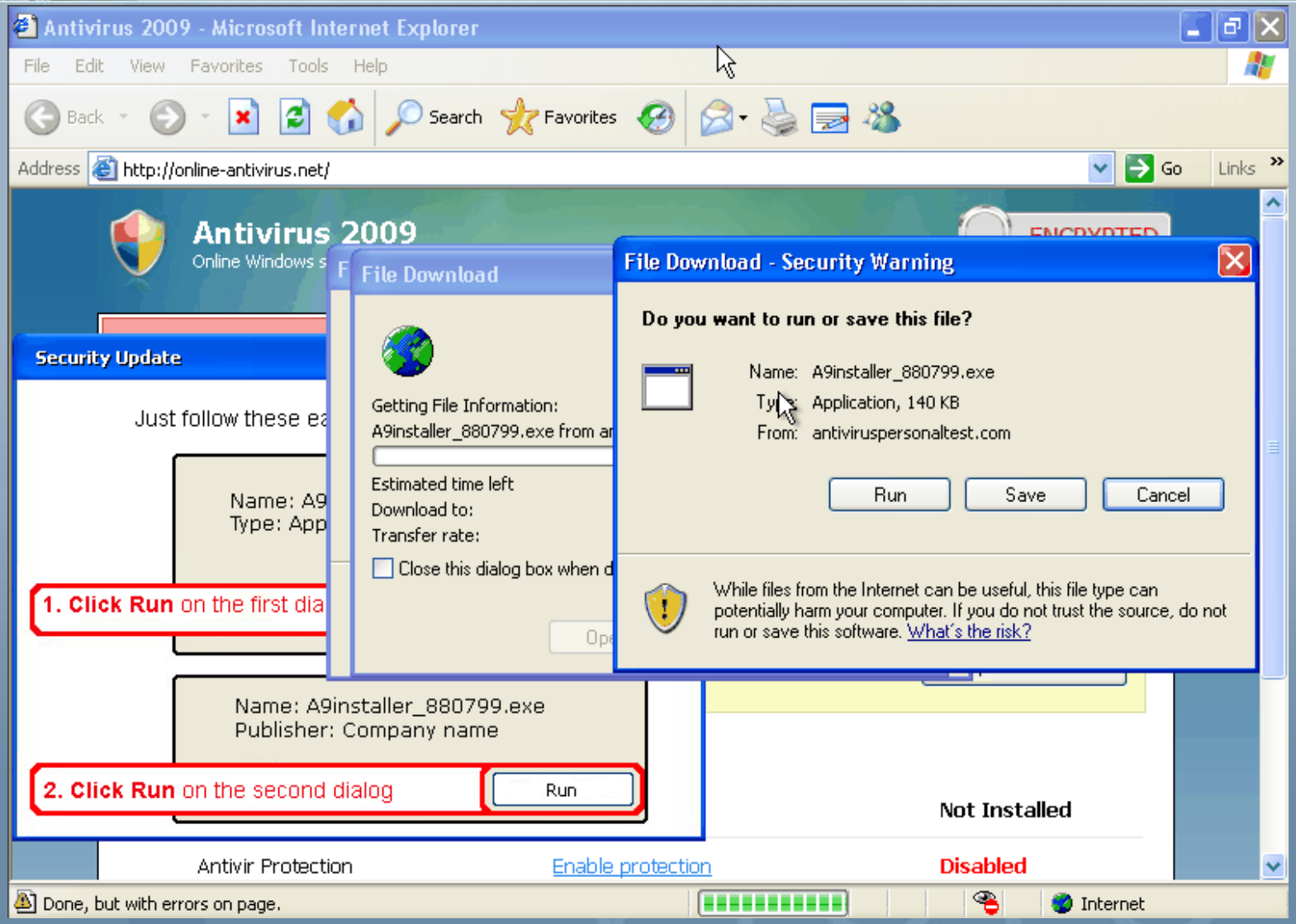
Suspicious emails

- Appear to come from your bank or someone you know
- Might ask you to make a phone call
- Might include official looking logos
- Phrases to watch out for:
  - Verify your account
  - You have won the lottery
  - If you don’t respond within 48 hours, your account will be closed

Suspicious links



Suspicious links



Spear Phishing

Computer Issue - Message (Plain Text)

Message | Developer

Reply | Reply to All | Forward | Delete | Move to Folder | Create Rule | Other Actions | Block Sender | Safe Lists | Not Junk | Categorize | Follow Up | Mark as Unread | Find | Related | Select

Respond | Actions | Junk E-mail | Options | Find

From: cio@wyo.gov
To: Crouch, Michael
Cc:
Subject: Computer Issue
Sent: Wed 3/10/2010 3:07 PM

Message | new-issues.txt (269 B)

Greetings,\n\nI have been recently experiencing issues with my computer and have been unable to run this report, I believe that the file may be messed up however, I cannot confirm this. Can someone please take a look and identify if it is my machine or just this file? I have an immediate deadline to produce this report, any help would be greatly appreciated.\n\nSincerely,\n\nJeff

new-issues.txt - Notepad

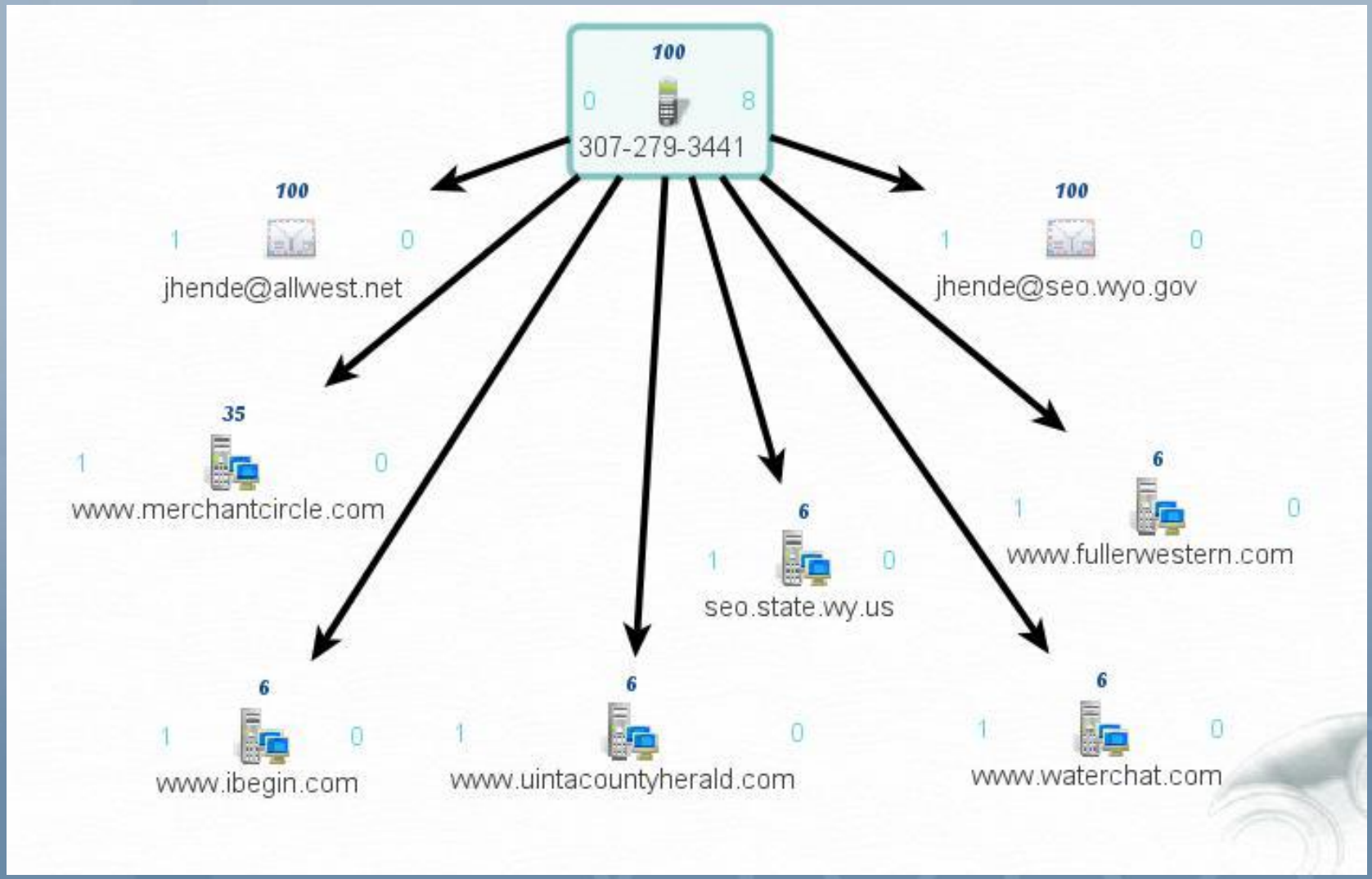
File Edit Format View Help

FILE QUARANTINED

Microsoft Forefront Protection for Exchange Server removed a file since it was found to be infected.
File name: "new-issues.pdf"
Malware name: "Win32/Swrort.A"

vision

Personal data



Personal data

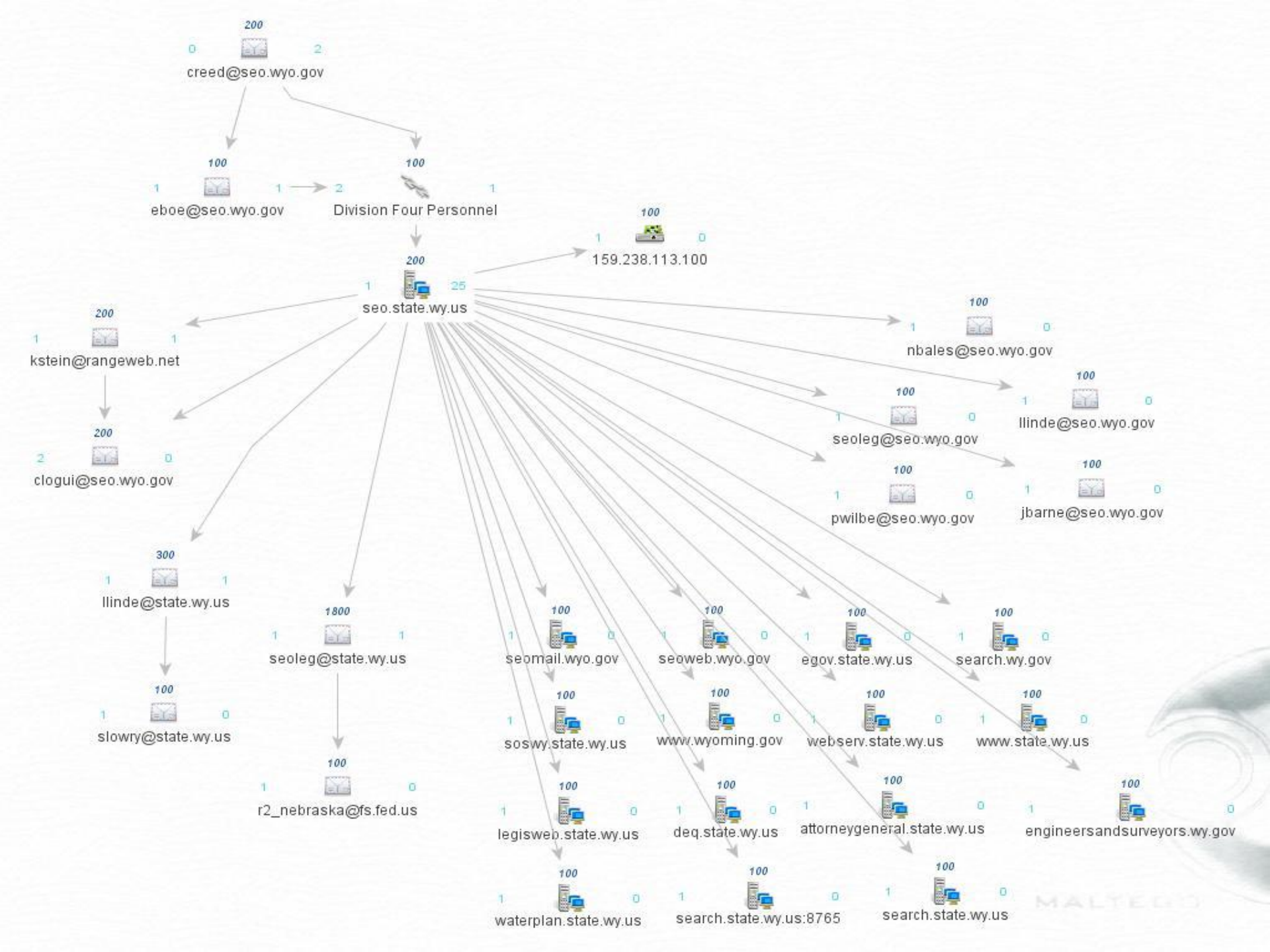
DIVISION IV: PERSONNEL AT LARGE

TITLE	NAME	ADDRESS
Superintendent	Jade Henderson, jhende@allwest.net, jhende@seo.wyo.gov	PO Box 277 Cokeville, Wyoming 83114
Assistant Superintendent	Kevin Payne kpayne@allwest.net kpayne@seo.wyo.gov	PO Box 277 Cokeville, Wyoming 83114
Administrative Spec. 3	Carol Reed, creed@seo.wyo.gov creed@allwest.net	PO Box 277 Cokeville, Wyoming 83114

DIVISION IV: WATER ADMINISTRATION PERSONNEL

DISTRICT	TITLE	NAME	ADDRESS
2,4,8,12	AS	Kevin Payne kpayne@allwest.net kpayne@seo.wyo.gov	PO Box 277 Cokeville, Wyoming 83114
1,3,9,14,15	LHC	John Yarbrough, jyarbr@seo.wyo.gov	PO Box 1208 Lyman, Wyoming 82937
5,6,7,10,11 ,13,16	LHC	Ed Boe eboe@centurytel.net eboe@seo.wyo.gov	PO Box 1080 Big Piney, Wyoming 83113
2	HC	Mike Johnson mjohns@allwest.net mjohns@seo.wyo.gov	PO Box 277 Cokeville, WY 83114

vision


creed@seo.wyo.gov
eboe@seo.wyo.gov
Division Four Personnel
159.238.113.100
seo.state.wy.us
kstein@rangeweb.net
clogui@seo.wyo.gov
nbales@seo.wyo.gov
llinde@seo.wyo.gov
seoleg@seo.wyo.gov
pwilbe@seo.wyo.gov
jbarne@seo.wyo.gov
llinde@state.wy.us
slowry@state.wy.us
seoleg@state.wy.us
r2_nebraska@fs.fed.us
seomail.wyo.gov
seoweb.wyo.gov
egov.state.wy.us
search.wy.gov
soswy.state.wy.us
www.wyoming.gov
webserv.state.wy.us
www.state.wy.us
legisweb.state.wy.us
deq.state.wy.us
attorneygeneral.state.wy.us
engineersandsurveyors.wy.gov
waterplan.state.wy.us
search.state.wy.us:8765
search.state.wy.us

Personal data

- Would you walk up to a complete stranger and tell them:
  - Bank account info
  - SSN / mothers maiden name
  - Credit card numbers
  - Email address
  - Phone number
  - Home address
- Then rethink posting this online

Social Engineering (avoidance)

- Be suspicious of unsolicited emails, phone calls or visitors
- Do not reveal or provide personal, organizational, or financial information to unauthorized individuals or in emails
- Don't send sensitive information over the Internet before checking a website's security

Social Engineering (avoidance)

- Pay attention to the URL of a website
- Try to verify email legitimacy by contacting the sender directly
- Install and maintain anti-virus software, firewalls, and email filters
- Take advantage of any anti-phishing features offered by your email client and web browser.

Social Media/Networks

Social Media/Networks (work)

Position of the Chief Information Officer – Not Yet

- Justifiable business ***need***
- Return on Investment (ROI)
- Terms of Service (TOS)
- Security risks and Privacy concerns
- Policies, Standards & Guidelines
- Official Agency position / Properly vetted

Social Media/Networks (personal)

Created with sharing in mind NOT privacy or security

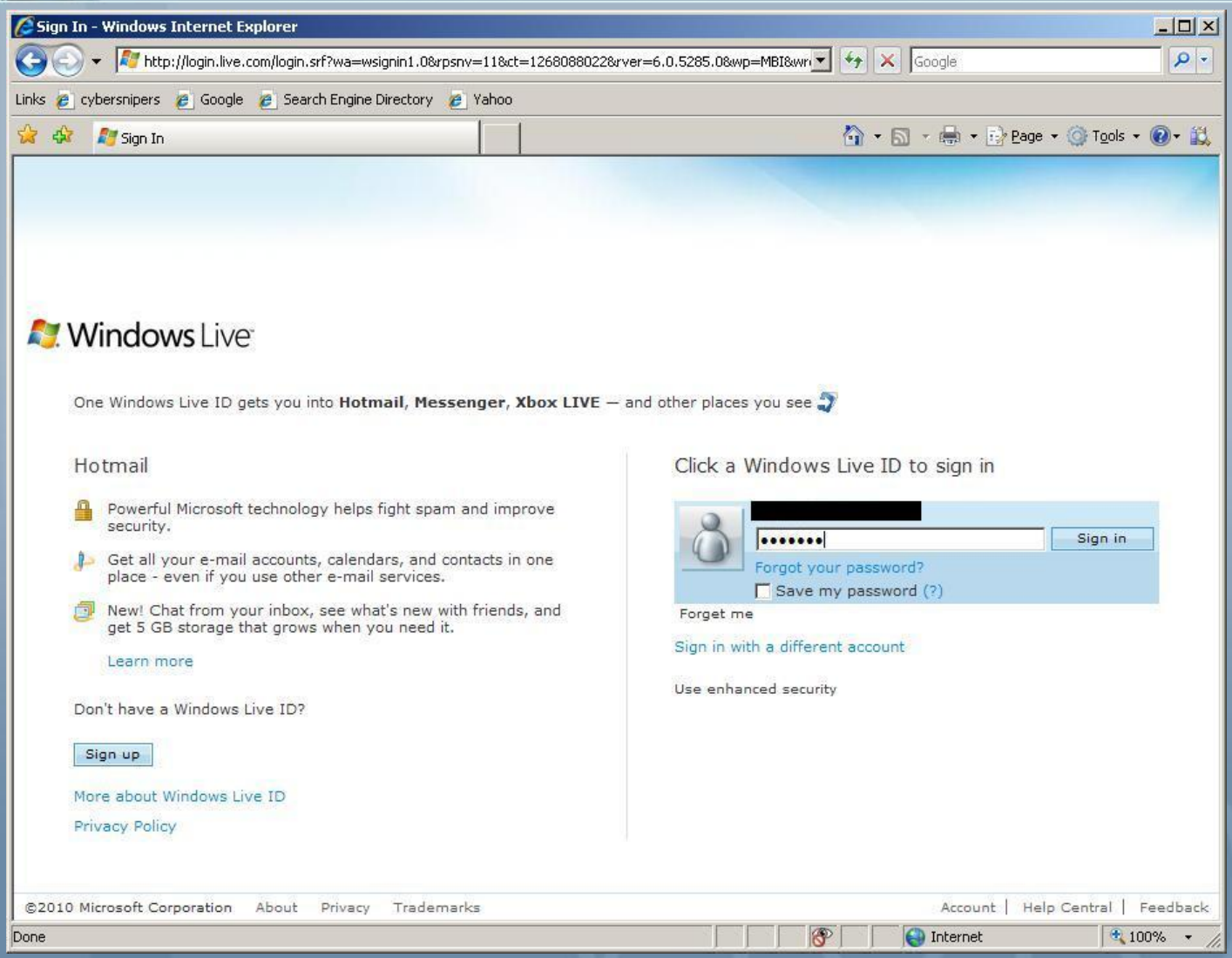
- Use your "Friends List"
- Remove yourself from search results
- Make your contact information private
- Keep your friendships private

Do **NOT** mix personal and professional posts

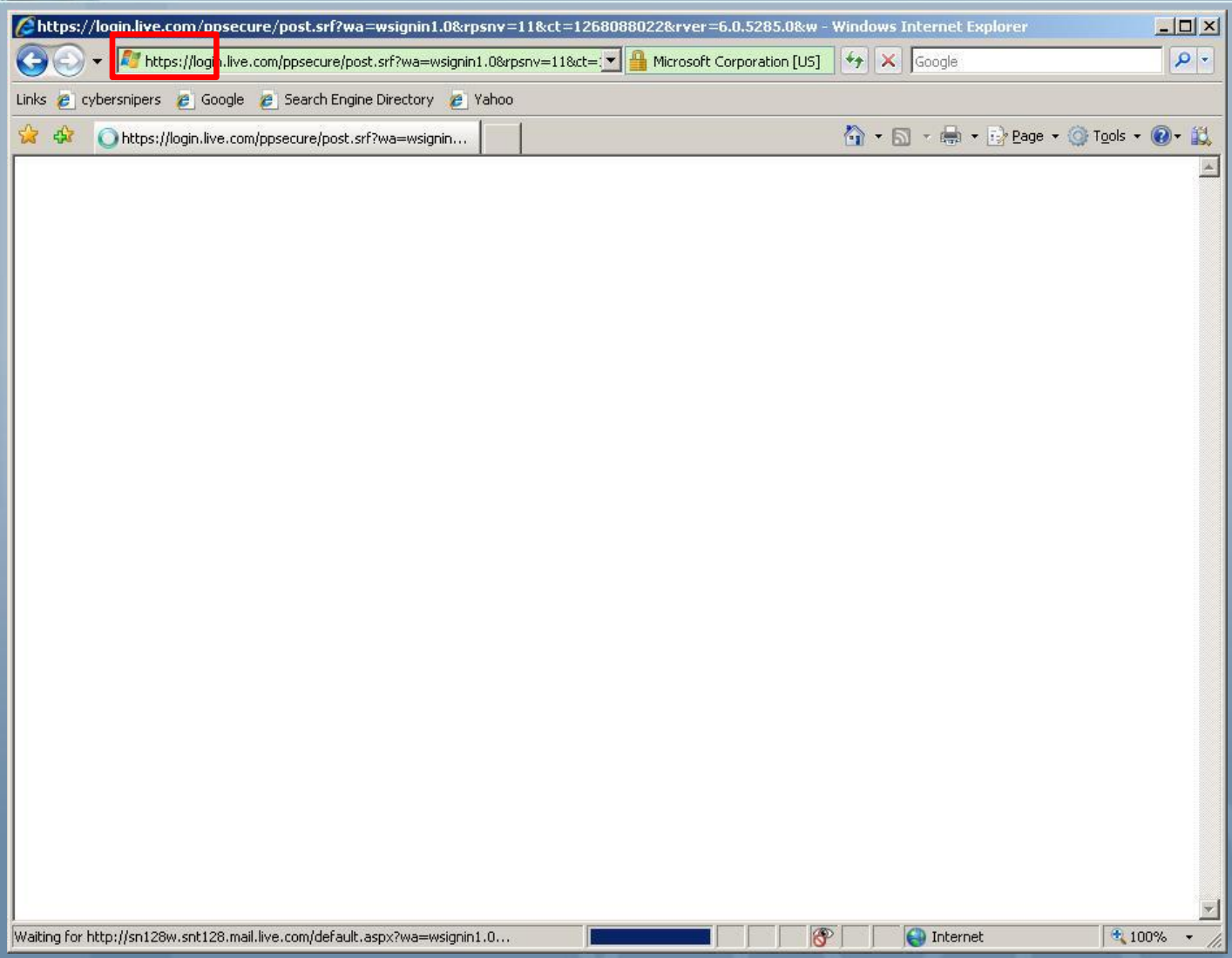
Encrypted Protocols

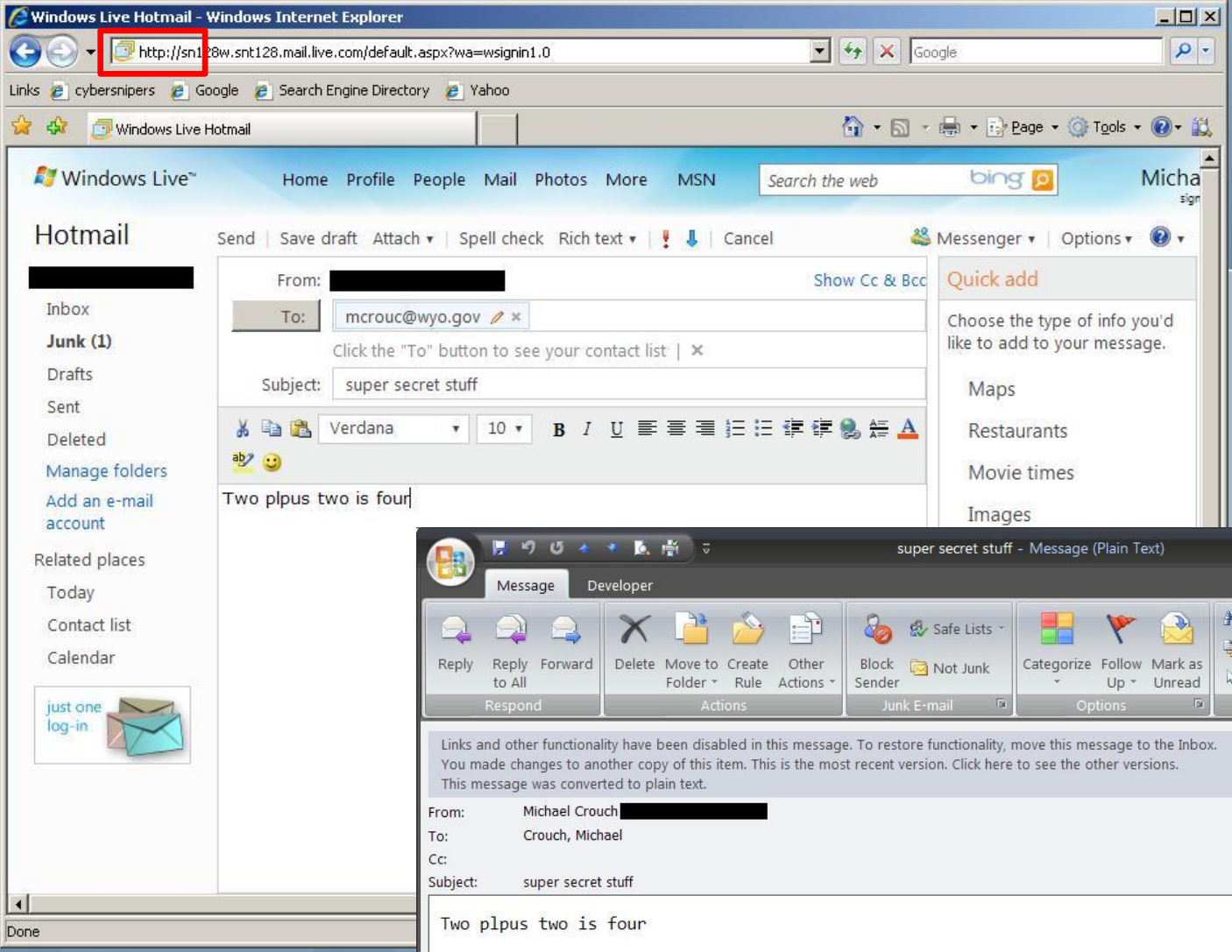
- Virtual Private Network (VPN)
- Transport Layer Security/Secure Sockets Layer (TLS/SSL)
- Hypertext Transfer Protocol Secure (HTTPS)
- FTP Secure or FTP-SSL (FTPS)
- Secure Shell (SSH)
- SSH FTP (SFTP)

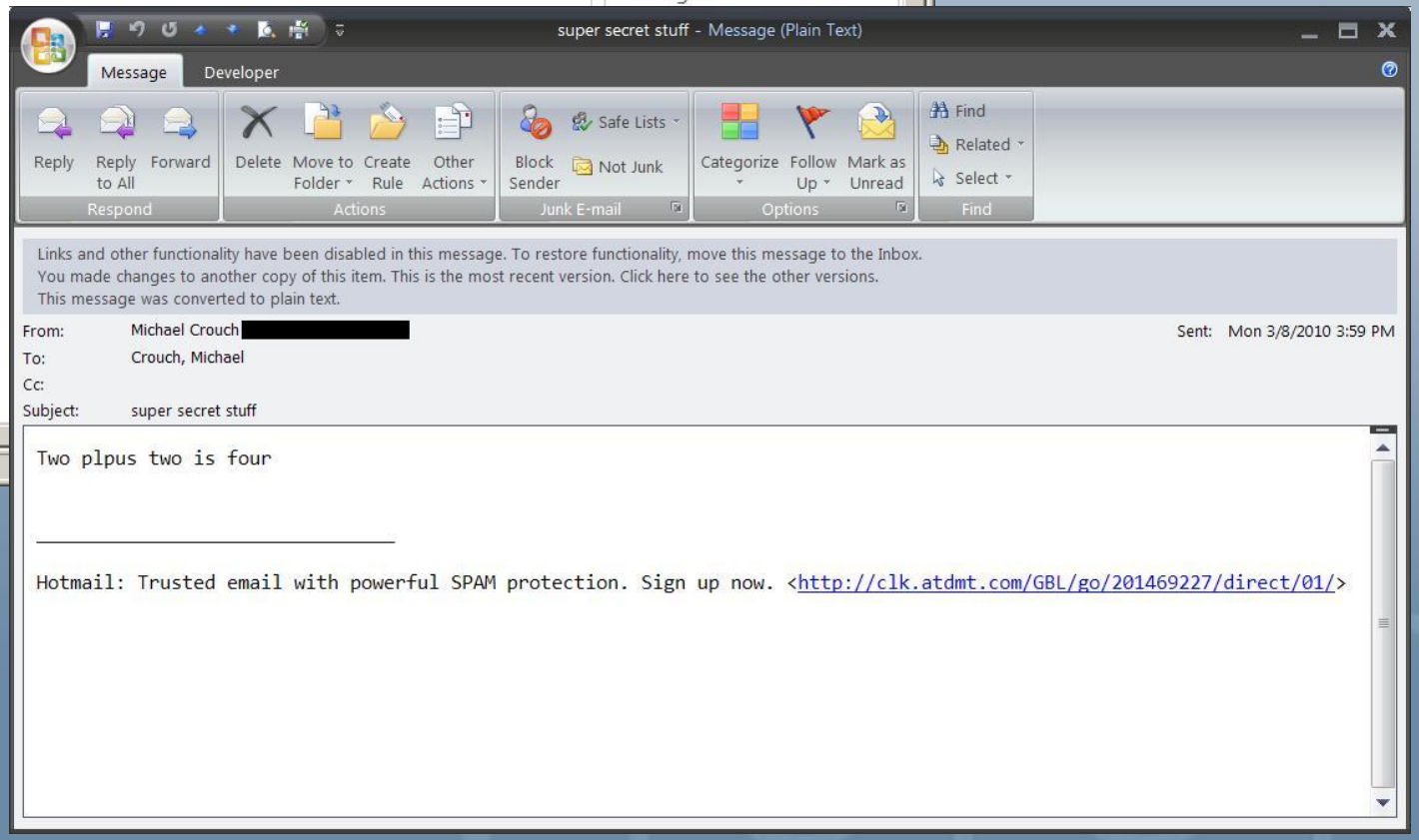
Encrypted Protocols



Encrypted Protocols

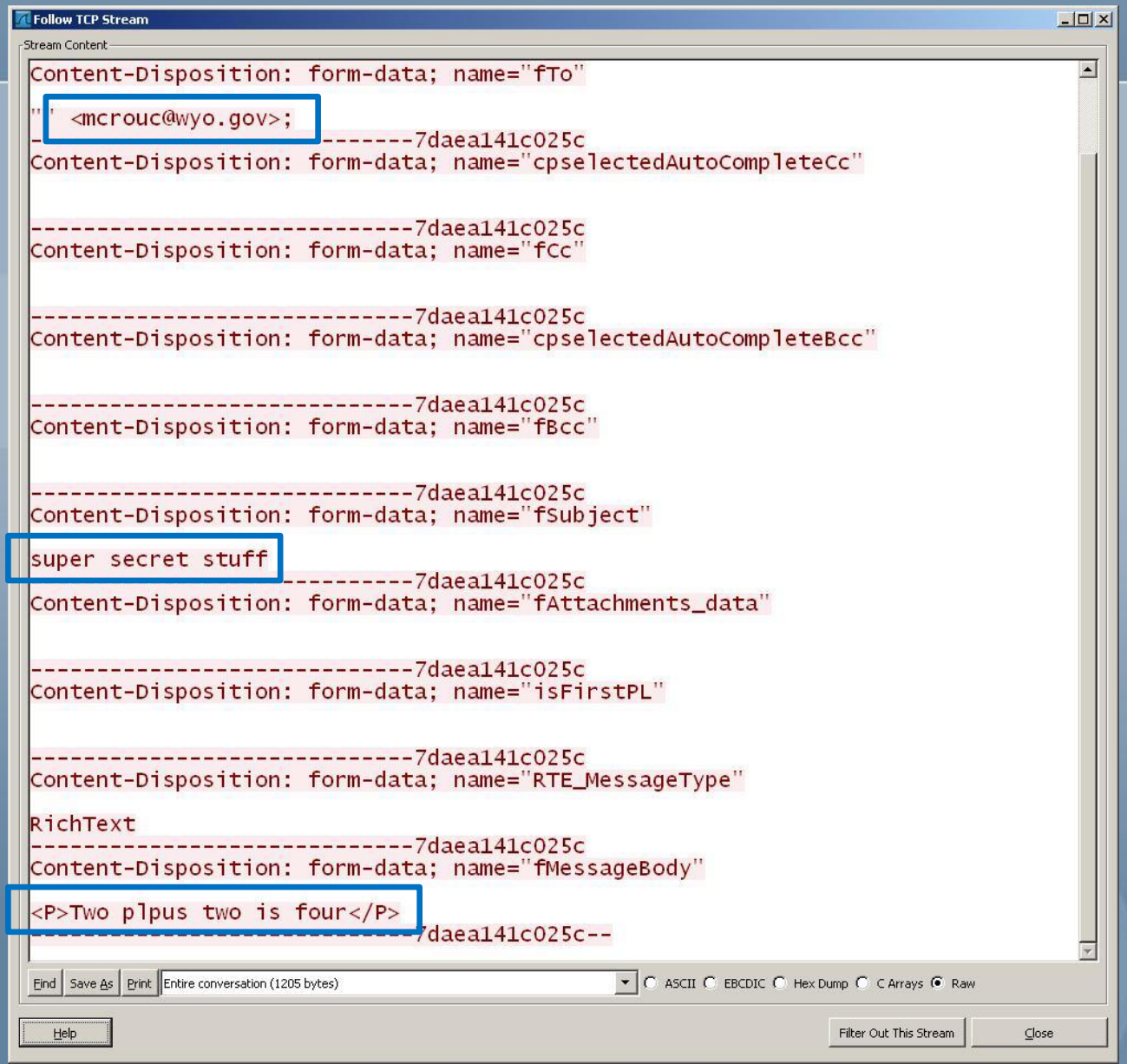



Windows Live Hotmail - Windows Internet Explorer
http://sn128w.snt128.mail.live.com/default.aspx?wa=wsignin1.0
Google
Links cybersnipers Google Search Engine Directory Yahoo
Windows Live Hotmail
Page Tools
Windows Live
Home Profile People Mail Photos More MSN
Search the web bing
Micha
sign
Hotmail
Send Save draft Attach Spell check Rich text Cancel
Messenger Options
[redacted]
Inbox
Junk (1)
Drafts
Sent
Deleted
Manage folders
Add an e-mail account
Related places
Today
Contact list
Calendar
just one log-in
From: [redacted]
Show Cc & Bcc
To: mcrouc@wyo.gov
Click the "To" button to see your contact list
Subject: super secret stuff
Verdana 10
Two plpus two is four
Quick add
Choose the type of info you'd like to add to your message.
Maps
Restaurants
Movie times
Images
Done


super secret stuff - Message (Plain Text)
Message Developer
Reply Reply to All Forward
Delete Move to Folder Create Rule Other Actions
Block Sender Safe Lists Not Junk
Categorize Follow Up Mark as Unread
Find Related Select
Respond Actions Junk E-mail Options Find
Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
You made changes to another copy of this item. This is the most recent version. Click here to see the other versions.
This message was converted to plain text.
From: Michael Crouch [redacted]
Sent: Mon 3/8/2010 3:59 PM
To: Crouch, Michael
Cc:
Subject: super secret stuff
Two plpus two is four
Hotmail: Trusted email with powerful SPAM protection. Sign up now. <http://clk.atdmt.com/GBL/go/201469227/direct/01/>

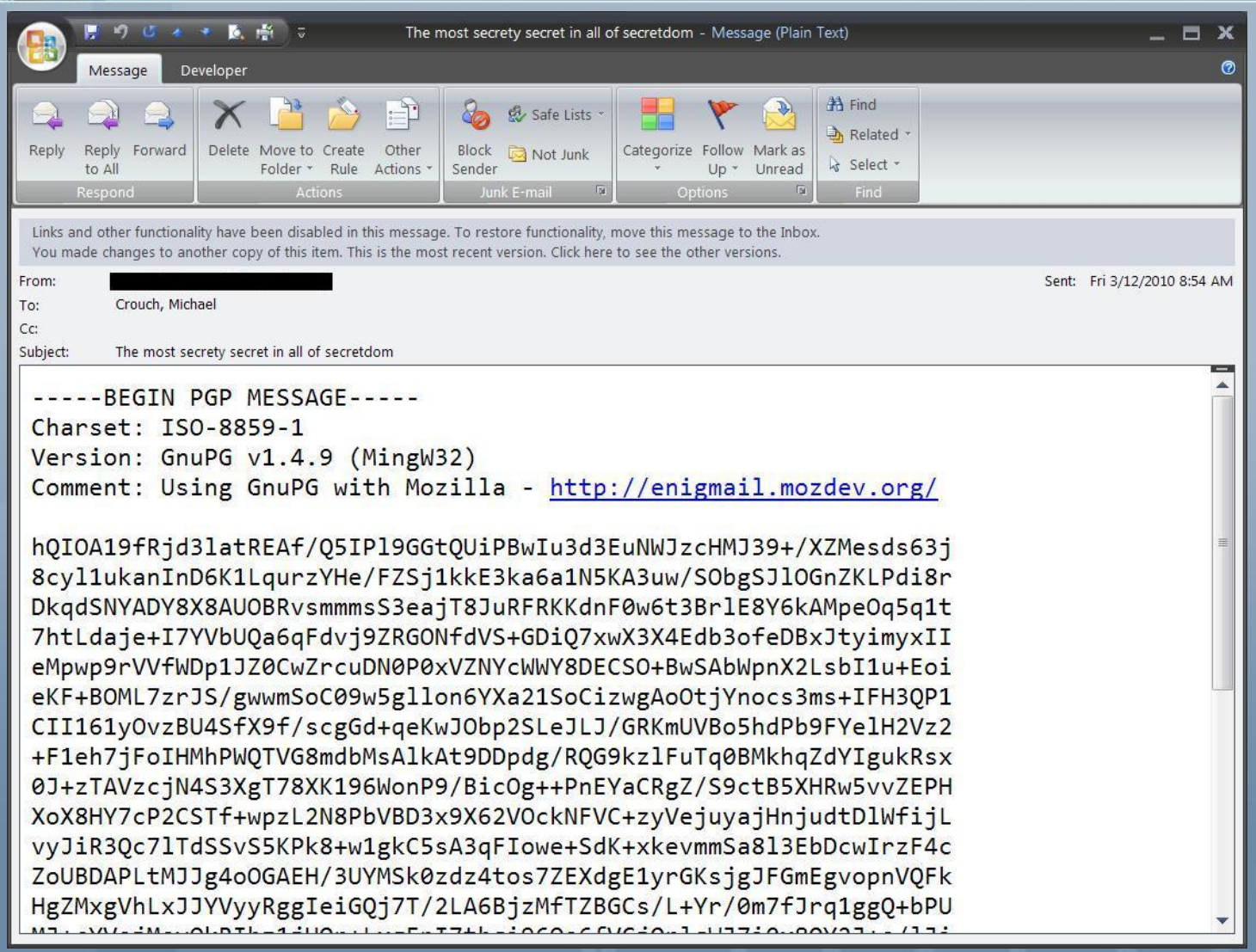
vision

Encrypted Protocols

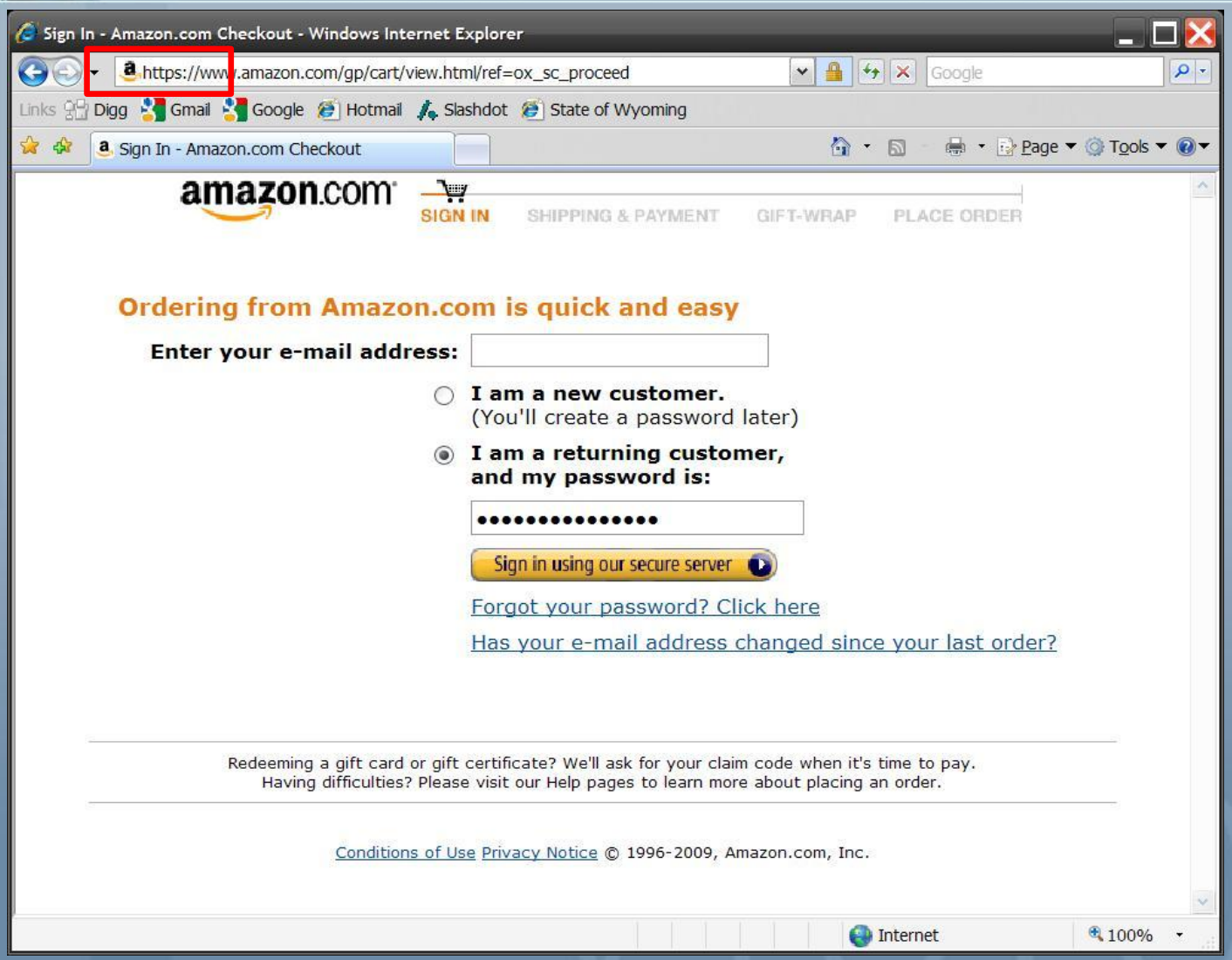


vision

Encrypted Protocols



Encrypted Protocols



Encrypted wireless

8 0.162603 00:24:01:36:a0:56 ff:ff:ff:ff:ff:ff IEEE 802.11 Beacon frame, SN=908, FN=0, Flags=.....C, BI=100, SSID="Emer214A"

```
Frame 8 (290 bytes on wire, 290 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 Beacon frame, Flags: .........C
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
  Tagged parameters (224 bytes)
    SSID parameter set
      Tag Number: 0 (SSID parameter set)
      Tag length: 8
      Tag interpretation: Emer214A: "Emer214A"
    Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 9.0 12.0 18.0
    DS Parameter set: Current Channel: 2
    Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    Country Information: Country Code: US, Any Environment
    Power Constraint: Tag 32 Len 1
    ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    RSN Information
      Tag Number: 48 (RSN Information)
      Tag length: 24
      Tag interpretation: RSN IE, version 1
      Tag interpretation: Multicast cipher suite: TKIP
      Tag interpretation: # of unicast cipher suites: 2
      Tag interpretation: Unicast cipher suite 1: AES (CCM)
      Tag interpretation: Unicast cipher suite 2: TKIP
      Tag interpretation: # of auth key management suites: 1
      Tag interpretation: auth key management suite 1: PSK
      RSN Capabilities: 0x0000
    Extended Supported Rates: 24.0 36.0 48.0 54.0
    Vendor Specific: 00:50:f2: WME
    Vendor Specific: 00:90:4c: HT Capabilities (802.11n D1.10)
    HT Capabilities (802.11n D1.10)
    Vendor Specific: 00:90:4c: HT Additional Capabilities (802.11n D1.00)
    HT Information (802.11n D1.10)
    Vendor Specific: 00:03:7f
```

```
0000  00 00 1a 00 6f 18 00 00  4f a1 56 72 02 00 00 00   ....o... O.Vr....
0010  10 02 6c 09 a0 00 b8 a9  00 0f 80 00 00 00 ff ff   ..l..... ........
0020  ff ff ff ff 00 24 01 36  a0 56 00 24 01 36 a0 56   .....$.6 .V.$.6.V
0030  c0 38 80 71 8c 89 01 00  00 00 64 00 31 05 00 08   .8.q.... ..d.1...
0040  45 6d 65 72 32 31 34 41  01 08 82 84 8b 96 0c 12   Emer214A ........
```

Public (open) wireless

```
1 0.000000 00:25:45:35:b8:47 ff:ff:ff:ff:ff:ff IEEE 802.11 Beacon frame, SN=2926, FN=0, Flags=.....C, BI=102, SSID="WyoPublic", Name="AP0022.9091.33f"
Frame 1 (267 bytes on wire, 267 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
  Tagged parameters (201 bytes)
    SSID parameter set
      Tag Number: 0 (SSID parameter set)
      Tag length: 9
      Tag interpretation: WyoPublic: "WyoPublic"
    Supported Rates: 1.0(B) 2.0(B) 5.5(B) 6.0 9.0 11.0(B) 12.0 18.0
    DS Parameter set: Current Channel: 1
    Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    Country Information: Country Code: US, Any Environment
    QBSS Load Element
    ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    HT Capabilities (802.11n D1.10)
    Extended Supported Rates: 24.0 36.0 48.0 54.0
    HT Information (802.11n D1.10)
    Cisco CCX1 CKIP + Device Name
      Tag Number: 133 (Cisco CCX1 CKIP + Device Name)
      Tag length: 30
      Tag interpretation: Unknown + Name: AP0022.9091.33f #Clients: 1
    Cisco Unknown 96: Tag 150 Len 6
    Vendor Specific: 00:40:96: Aironet Unknown
    Vendor Specific: 00:40:96: Aironet CCX version = 5
    Vendor Specific: 00:40:96: Aironet Unknown
    Vendor Specific: 00:40:96: Aironet Unknown
    Vendor Specific: 00:50:f2: WME

0000  00 00 1a 00 6f 18 00 00  24 26 54 72 02 00 00 00   ....o... $&Tr....
0010  10 02 6c 09 a0 00 cb a9  00 22 80 00 00 00 ff ff   ..l..... ."......
0020  ff ff ff ff 00 25 45 35  b8 47 00 25 45 35 b8 47   .....%E5 .G.%E5.G
0030  e0 b6 78 f1 ca 3c 07 01  00 00 66 00 21 04 00 09   ..x..<.. ..f.!...
0040  57 79 6f 50 75 62 6c 69  63 01 08 82 84 8b 0c 12   WyoPubli c.......
```

Public (open) wireless

153 8.132254 192.168.0.116 74.125.47.138 HTTP GET /generate_204 HTTP/1.1

```
Frame 153 (781 bytes on wire, 781 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol, Src: 192.168.0.116 (192.168.0.116), Dst: 74.125.47.138 (74.125.47.138)
Transmission Control Protocol, Src Port: 3023 (3023), Dst Port: 80 (80), Seq: 6285, Ack: 4369, Len: 677
Hypertext Transfer Protocol
GET /generate_204 HTTP/1.1\r\n
Accept: */*\r\n
Referer: http://www.google.com/search?hl=en&source=hp&fkt=3141&fsdt=7266&q=wireless+capture&aq=f&oq=&aqi=g
Accept-Language: en-us\r\n
UA-CPU: x86\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Info
Host: clients1.google.com\r\n
Connection: Keep-Alive\r\n
[truncated] Cookie: PREF=ID=2dacaed2530a6edb:U=416f0ef6e1fb5991:TM=1258987765:LM=1258993588:GM=1:S=KVREsbV
\r\n
```

```
0000  00 00 1a 00 6f 18 00 00  e0 67 b2 e3 01 00 00 00   ....o... .g......
0010  10 d0 6c 09 c0 00 e0 aa  00 36 88 01 30 00 00 25   ..l..... .6..0..%
0020  45 35 b8 47 00 21 5c 52  bf 2b 00 15 05 9a 57 2c   E5.G.!\R .+....W,
```

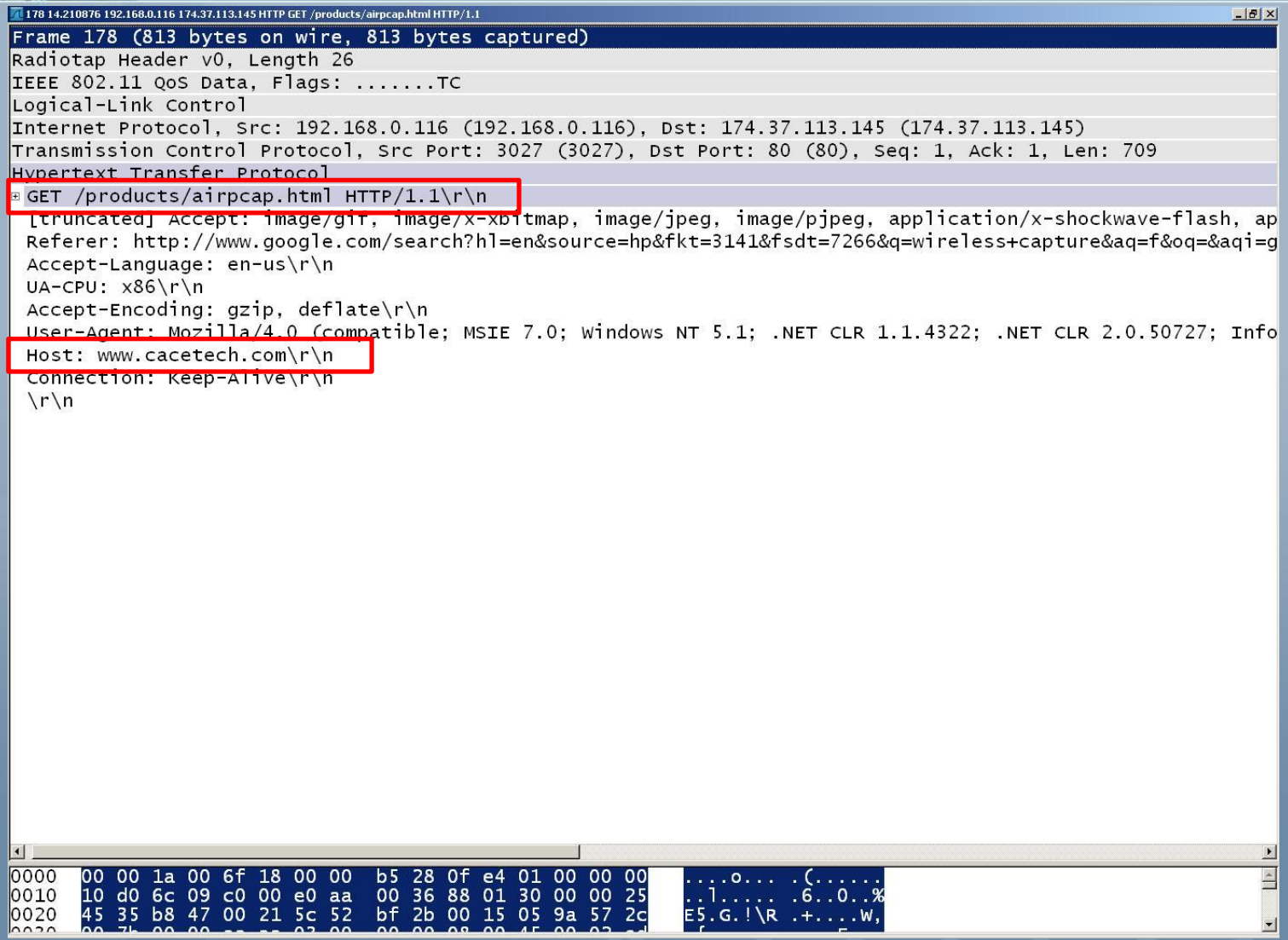
Public (open) wireless

http%3A%2F%2Fwww.cacetech.com%2Fproducts%2Fairpcap.html

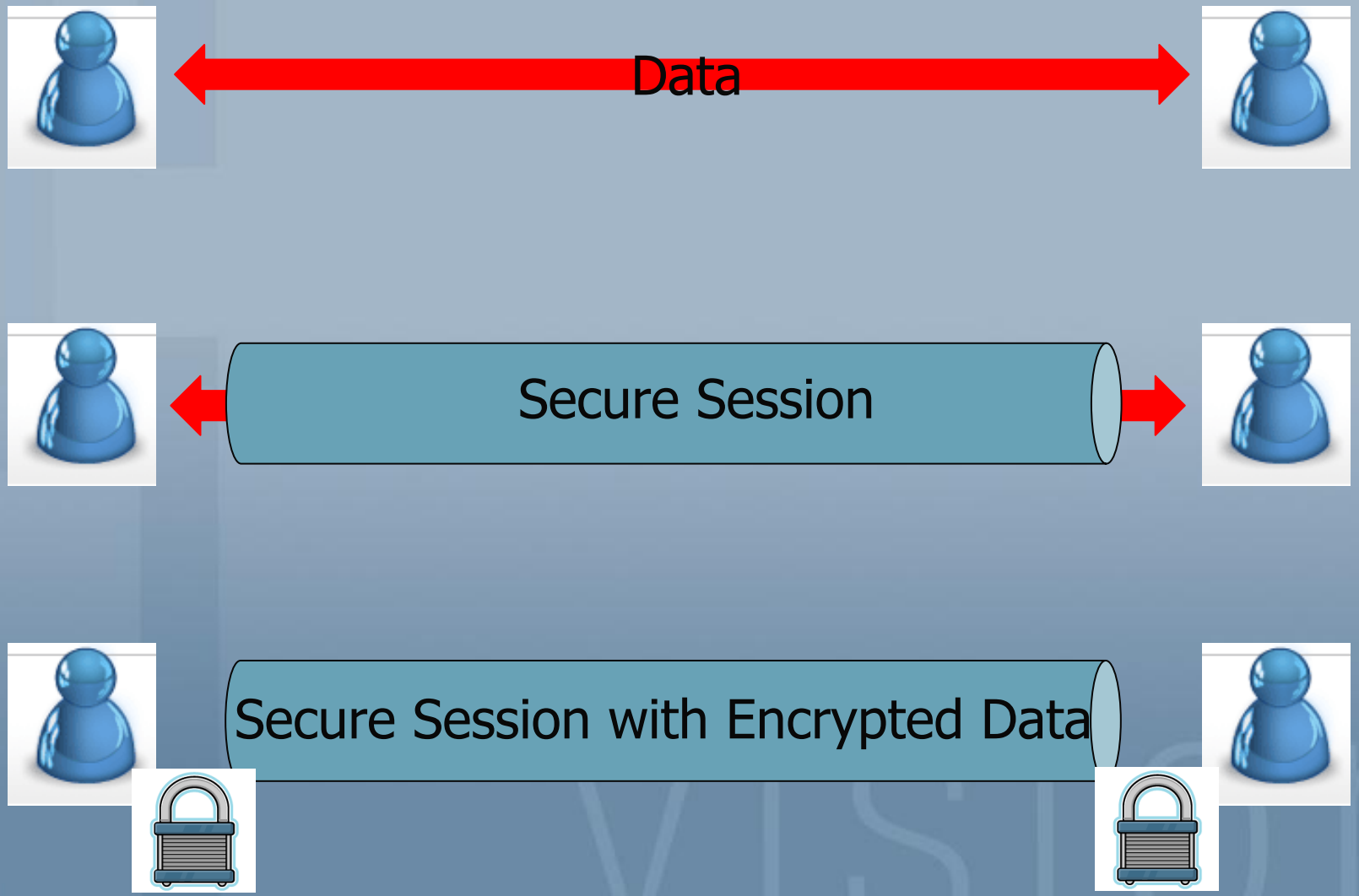
=

http://www.cacetech.com/products/airpcap.html

Public (open) wireless



Secure Communications



Passwords

- Alpha-numeric, special characters
- 9-15 characters long (or more)
- Change every 60 days or sooner
- Don’t recycle passwords too often
- Different account; different password
- Use a password manager/safe

Passwords

- 09Rockie$
- 1337 $kilz
- !P@s$W0rD
- 1234567890
- 1Q2W3E4R
- z!x@c#v$
- ???????

Took 10 minutes to crack these passwords

Passwords

- M3t@b0l!sm
- §3cReT$

mary had a little lamb, its fleece was white as snow

- mhallifwwas
- MhA1l!fwW@s

Data backups

- Easy and inexpensive to perform
- Difficult and costly to replace

- 64 GB of storage $135

- 250 GB of storage $100

- 1 TB of storage as low as $90

Data backups

- Lots of applications on the market
- Consider a full disk image to backing up data
- Label your backup media or images
  - Date of backup/image
  - What's on it
- Store backups in a safe location
  - Fire proof box or safe
  - Off-site is best-practice

Defense-in-Depth

QUESTIONS